

**North Carolina State Government
Statewide Initiatives and Strategies
2003-2005 Biennium**

**State CIO's Recommended
Approach for Managing Information
Technology for a Better North
Carolina**

Supplemental Materials

December 19, 2002

**North Carolina State Government
Statewide Initiatives and Strategies
2003-2005 Biennium**

Supplemental Materials

Table of Contents

PURPOSE AND EXPLANATION	4
CHAPTER 1 TECHNOLOGY OVERVIEW	5
PRESENT ROLE AND IMPORTANCE OF IT.....	5
POTENTIAL VALUES AND BENEFITS TO STATE GOVERNMENT	6
DEFINING CHARACTERISTICS AND MANAGEMENT ISSUES.....	7
MAJOR TRENDS AND FUTURE CONSIDERATIONS.....	8
CHAPTER 2 GOVERNANCE OF INFORMATION TECHNOLOGY IN STATE GOVERNMENT	11
OVERVIEW OF GOVERNANCE IN GENERAL	11
DOMAINS OF GOVERNANCE.....	12
OVERVIEW OF GOVERNANCE FOR THE STATE.....	13
HISTORICAL PERSPECTIVE OF GOVERNANCE FOR THE STATE.....	15
CHAPTER 3 ANALYSIS OF AGENCY EXPANSION BUDGET REQUESTS (ATTACHMENT CS).....	17
CHAPTER 4 – ANALYSIS OF AGENCY IT PLANS.....	21

Acronyms:

CIO	Chief Information Officer
CJIN	Criminal Justice Information Network
HIPAA	Health Insurance Portability and Accountability Act
IRMC	Information Resource Management Commission
IT	Information Technology
ITMAC	Information Technology Management Advisory Committee
ITS	Information Technology Services
LAN	Local Area Network
PC	Personal Computer
QA	Quality Assurance
TCP/IP	Telecommunications Control Protocol/Internet Protocol
WAN	Wide Area Network

Purpose and Explanation

This is a companion document to the *Statewide Initiatives and Strategies, 2003-2005 Biennium – State CIO's Recommended Approach for Managing Information Technology for a Better North Carolina*. It offers background and explanatory information that supports the facts, initiatives, and strategies of the lead document.

Chapter 1 Technology Overview

Present Role and Importance of IT

IT is pervasive. It impacts the growth and prosperity of our state, the health and welfare of our citizens, the vitality of our economy, the profitability and long-term viability of our industries, and the conduct of our democratic processes. It dictates the techniques, methods and procedures of business transactions, public services, and private interactions. Along with political, sociological, and economical influences, it is a key contributor to our standard of living and the ways we work and play.

While IT has advanced tremendously from the first computers in the 1940s, to the mainframes of the 1950s and 1960s, the PCs of the 1970s and 1980s, and the Internet and portable devices of the 1990s and 21st century, it is still continuing to advance even more rapidly. The convergence of technologies for computing, data storage and telecommunications has enabled the collection, manipulation and dissemination of vast amounts of information from the three perspectives of “anytime”, “anywhere”, and “anyway”.

To date, the major uses of IT have been to automate business processes and to provide faster access to more useful information. The investments in IT have resulted in the achievement of productivity increases, creation of new industries, changing of business models, providing of new products and services, gaining of new customers, and revolutionizing of the interaction among suppliers and customers.

In the private sector, a new lexicon for business success factors has been created. Competitive advantage is now determined by considerations directly linked to the organization’s ability to employ and manage IT successfully. These include:

- Improved customer service through speed of delivery; choice of models, sizes, types, etc.; convenience of interaction (e.g., self-service); and personalization of interaction to fit individual preferences and desires.
- Better quality of products or services through increased functionality or capabilities, more reliability, easier to use, etc.

- Greater employee efficiency and effectiveness through process redesign, better teamwork, additional collaboration, availability of more timely and useful information, etc.
- Increased service value and reputation through better and more customer-centric products and services, competitive new or enhanced offerings, and clearly recognized excellence in customer care.
- Improved connectedness of partners, suppliers and customers through the sharing of essential information in a timely manner to meet quality specifications, delivery deadlines and service level expectations.

Potential Values and Benefits to State Government

Technology is big business in North Carolina's state government. In fiscal year 2001-2002, state agencies spent more than \$700 million on technology. This number does not include public schools, community colleges, or local governments. State agencies – including UNC – employ more than 5,000 employees in technology positions, and the average salary is approximately \$58,000.

Like the private sector, state government is facing the daunting challenges presented by the stagnating economic environment; the threat of terrorism; expanding federal and legal mandates (such as HIPAA); and increasing expectations of the public for faster and more convenient services provided more efficiently. State government is using technology to confront these situations and to transform the way it does business.

Since IT is an inextricable part of how state government functions, it has the potential for offering the following advantages to the public:

- Facilitating easier access to and more responsive interaction with state entities by offering a consistent and coherent view of government that crosses organizational boundaries and encourages collaboration among programs, state agencies, and local, state and federal governments; providing functional integration of mainstream services; offering a broad diversity of self-service capabilities that are accessible in a variety of ways, at anytime and from anywhere; and presenting a wide range of easy to research information in useful formats.

- Increasing productivity and improve efficiencies of business processes by automating tasks that were previously accomplished manually, eliminating logjams, and enabling changes in workflows that streamline operations and remove redundancies in work steps.
- Improving the value and benefits of governmental programs by supporting a focus on citizen-centric approaches and results-oriented outcomes.
- Contributing to educational opportunities, public safety and welfare, and economic development and quality of life by providing more useful and timely information and better support tools (which allow better decisions to be made at a faster pace and with more informed input) to the state's teachers, social workers, law enforcement officers, industry recruiters, health officials, highway designers, and other workers.

Defining Characteristics and Management Issues

The following principles are useful in the governance of statewide IT in that they serve as questions that agency senior managers and the state's central IT management or oversight bodies may want to ask as part of their responsibility for the integrity, health and performance of IT functions and operations:

- Do technology investments or assets enable the achievement of agency missions and the improved performance of business/program operations? – Technology projects should follow agency strategies and business/program initiatives so that business processes are conducted in an efficient and cost-effective manner, desired program outcomes or results are achieved, and expected citizen value and economic benefits are realized.
- Is the integrity of information preserved? – IT assets should be protected (in a cost-justified manner) from unauthorized access, sabotage, piracy, or natural disasters.
- Is citizen-centricity promoted? – E-government applications that feature a common view, self-service and convenience should receive priority attention for funding and implementation.

- Are applications developed and infrastructures implemented consistently within agency and statewide technical architectures? – Best practices and standards should be documented and followed, and variations should be allowed only for responsible and compelling exceptions.
- Are products vendor-neutral and products and services competitively bid? – Technology choices should be based on vendor-neutral standards, and best-value and performance-based procurements should be employed.
- Are we practicing the concepts of reusing before buying and buying before building? – Whenever possible, statewide shared infrastructures and common services should be used, and serious considerations should be given to purchasing applications before developing proprietary systems.
- Is technology managed as an investment? – New solutions or assets should be adopted where appropriate, cost-beneficial and within acceptable risk profiles; hardware/software products and communications equipment should be operated effectively and efficiently; and legacy investments should be retired or replaced when no longer cost-effective or risk-acceptable.
- Are the biggest risks related to the implementation and operation of technology identified and addressed aggressively in a proactive manner? – Risk management (i.e., the anticipation of risk factors, advance planning for avoidance of them, and focused attention to minimize repercussions from them) should be a primary component of the overall management of technology.

Major Trends and Future Considerations

Short-term business trends in IT are dictated by two major situations. First, the general economy is in decline, and the reversal, when it comes, will probably be uneven among geographic regions and sporadic in progression. Regarding state governments, only a very few are not experiencing severe budget shortfalls, and the total budget deficit for the states is estimated to be a combined \$58 billion according to a recent Wall Street Journal article. According to a report recently released by the National Governors Association, nearly every state is in fiscal crisis. North Carolina state government's fiscal situation is particularly perilous due to a confluence of adverse financial events arising from costly legal judgments; response to

hurricanes, floods, and snow and ice storms; increased costs for social services; growth in student enrollments; and deficiencies in tax revenue arising from the sluggish economy and the precipitous decline of the stock market. Record unemployment numbers have been experienced in many sectors, including textiles, manufacturing, high technology and telecommunications. Relief may be an extended time in coming, as the state transitions its economy from dependence on agriculture and textile and apparel manufacturing to one more diversified and reliant on services, finances, and trade.

Second, the tragedies of September 11, 2001, and the accompanying focus on security has restructured priorities and revised plans relative to IT in governments and private businesses. Along with the threats of potential physical, biological, chemical and nuclear terrorism, the IT community must address the adverse impacts of cyber terrorism. Moreover, citizens are demanding greater protections and assurances for individual privacy and confidentiality of data.

As a result, state technology leaders must position IT to:

- Cut costs and assist governmental programs to achieve operational savings and better outcomes.
- Deliver more value to the taxpayers from investments and do so in shorter time periods.
- Strengthen security infrastructures and expand disaster recovery and business continuity capabilities.
- Become more citizen-focused in decision-making.

Improved management, innovative thinking, and tighter control are the watchwords for today's IT business environment.

Severe budget constraints; rising citizen demands for quicker, better, and more responsive services; and public expectations for greater accountabilities for benefits and values from expenditures dictate that IT must be closer tied to the state's business processes and program operations. IT plans and budgets must be directly linked to business strategies and program goals and objectives. Potential investments must be justified by financial benefits, as well as political value.

Finally, IT initiatives must consider the following major challenges:

- Knowledge capital of the state's 250,000 plus employees, including public education.
- Asset management of the multitude of PCs, servers, laptops and other computing and communications devices in the state's inventory.
- Electronic government (e-government) for providing information, interactions, and services to citizens and employees in a self-service mode when and how they desire.
- Integration of the many databases and applications to present a single or consistent view of government and provide a one-stop experience for both the public and state workers.
- Mobile computing and ready access to information by state employees as they perform their responsibilities and duties throughout the vast expanse of the state's geographic boundaries.
- Security, privacy and confidentiality of information and reliability of operations, even under unfavorable conditions, to protect the state's vital data assets and ensure the availability of information when and where needed.

Chapter 2 Governance of Information Technology in State Government

Overview of Governance in General

Governance is the structure for making decisions, while management is the making of the decisions. The three main components of governance are (1) the scope or areas covered by decisions (such as policies, architecture, investment selections, etc.), (2) the decision-making mechanisms (processes, procedures, policies, committees, etc.), and (3) the assignment of decision-making authority, responsibility and accountability. These are the “what”, “how”, and “who” of governance. Good governance is required to obtain good decisions on a consistent basis. IT governance typically involves decisions in the five areas of policies/principles, strategy, investment selection and implementation, technical architecture, and quality assurance.

The three key success factors for good IT governance are:

- Fundamental IT principles, beliefs and values are known and agreed to.
- Decision-making responsibilities and authorities are clear and understood.
- Mechanisms for input and participation are in place, adequate, and used.

Successful governance in state government accomplishes the following two objectives:

- Make IT and the business/program areas jointly responsible and accountable for linking IT investments to the most important business/program strategies and goals of the state.
- Produce statewide-oriented IT decisions that satisfy governmental mandates, agency strategies and missions, and program goals and objectives in the most cost-effective manner.

The challenge for large organizations in both the public and private sectors is that from the perspective of individual entities and stakeholder groups, IT

issues are local, while governance from an enterprise perspective must persuade them that IT decisions should be made from a more global viewpoint in order for everyone to partake in the benefits while minimizing costs.

Domains of Governance

A major issue for IT governance is the scope of responsibility for IT decision making when multiple organizations with potentially conflicting interests are involved. For state government, this typically distills to who controls or owns what IT assets and associated policies and standards. It usually falls into one of three categories – individual agency, community of interest (such as human services, public safety, education, etc.), and central IT services organization (such as ITS).

As a general rule, the trend in both the public and private sectors is for IT assets and functions, which are not unique to the mission-critical functions of an agency or line of business, to be managed by central IT services entity. This trend is due to the greater economic benefits accruing from consolidated IT asset purchases and operations; the advantages for increased reliability, security, and flexibility from having a more robust IT infrastructure useable as a common resource by all; and the more competitive and challenging economic and business environments. The latter is putting intense pressure on business and governmental leaders to ensure (a) that the purchase, implementation, and operation of IT assets are performed in the most economical and cost-effective manner and (b) that these assets deliver the greatest possible benefits and value to funding parties (taxpayers and shareholders).

Properly managed and accounted for, a more centralized IT management structure offers the following advantages:

- Reduced operating and support costs from the greater degree of standardization of platforms and support/operating software.
- Greater economies of scale by aggregating purchases to obtain higher volume discounts and by spreading more transactions over fixed costs of assets to reduce unit costs of production (utility model).
- Consistent support and service and more reliable and secure operations for all applications and participating organizations from

the use of common technical services and shared technical infrastructure.

For most public entities and commercial sector organizations shifting to a more enterprise and utility model of IT management structure, the following items are owned, governed, and/or managed at the enterprise (statewide) level:

- Enterprise architecture.
- Enterprise quality assurance.
- Computing devices (especially mainframes and servers).
- Applications that are mission critical to the enterprise, such as core business systems (finance, budgeting, accounting, human resource, etc.).
- Standards for all assets (hardware, common software, data shared or exchanged within the enterprise, and telecommunications equipment).

Agencies or lines of business typically are responsible for IT items unique to their businesses or programs. These include individual architectures, applications, and data standards applicable only to them or their communities of interest.

Overview of Governance for the State

The political governance structure for North Carolina follows the typical state organization with legislative, judicial, and executive branches. The executive branch is composed of ten members of the Council of State elected by the citizens every four years. They include the Governor and the Lieutenant Governor. Eleven Executive Department Secretaries are appointed by the Governor and serve at his pleasure. The State Controller is appointed by the Governor and confirmed by the General Assembly for a seven-year term.

Over the years, the statewide governance of IT has evolved from almost complete autonomy and independence by the executive agencies to a more statewide focused approach or closer unity of federated entities featuring the Information Resource Management Commission as a top-level coordinating and policy-making body and a State CIO reporting to the Governor. The

legislative branch has its own IT management structure separate from the others. The judicial branch also is independent; however, its chief administrative officer (Director, Administrative Officer of the Courts) is a member of the IRMC, and its technology plans must be reviewed by the IRMC. Similarly, the University System is represented on the IRMC, but it is not under the policies of the IRMC.

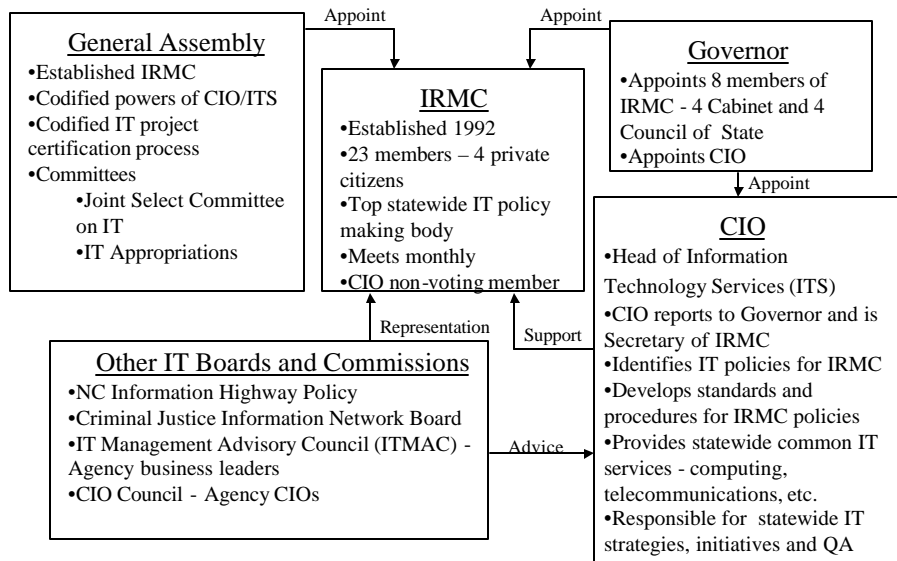
For the executive branch, each department and agency is responsible planning and managing its IT functions, including funding requests, budgeting, staffing, implementation projects, and operations of assets and technical infrastructures. The 23-member IRMC has broad-based statewide IT policy-making duties in the areas of planning, operations, quality assurance, and purchasing. The Governor appoints eight members of the IRMC. The State CIO is Secretary to the IRMC, but is not a voting member.

The State CIO is the head of the central IT service providing organization (ITS). He identifies policies for the IRMC, develops statewide standards and procedures to carry out IRMC policies, assists the IRMC in the performance of quality assurance functions, has statewide-level security responsibilities, performs IT purchasing through statewide term and convenience contracts and approval of agency purchase documentation, and prepares recommendations for the IRMC's biennial Statewide Initiatives and Strategies document.

The IT Management Advisory Council (ITMAC) is composed of state business leaders and has a representative on the IRMC. The CIO Council is composed of agency IT heads, and meets monthly to provide advice to the State CIO. Other IT boards and commissions include the NC Information Highway Policy Committee and the Criminal Justice Information Network (CJIN) Board.

The General Assembly has codified the powers and duties of the IRMC and the State CIO/ ITS. It has a Joint Select Committee on IT and House and Senate IT Appropriations Committees. A key statute governing statewide IT is G.S. 143-48.3. The chart below highlights the statewide IT governance structure.

North Carolina State Government
Information Technology Management
Statewide Governance Structure



Historical Perspective of Governance for the State

The chart below highlights the major events in recent history impacting the governance structure for the management of IT in state government.

Time Period or Event	Title of Period or Event	Description of Major Results or Outcomes
Late 1950s to early 1980s	Autonomous operations	<ul style="list-style-type: none"> • Weak statewide governance • Little or no sharing of IT infrastructure • Disparate availability and use of technology among agencies
1983	Establishment of central services organization (SIPS)	<ul style="list-style-type: none"> • Mainframe consolidation, with sharing of computing power, support staff and software • SNA network implementation and consolidation of major independent agency networks
Early 1980s to early 1990s	Best value IT for legacy architecture	<ul style="list-style-type: none"> • Reduce unit cost of computing and telecommunications • Raise the level of technology available to all agencies • Improve information sharing among programs and agencies • Improve IT infrastructure for state government
1992	IRMC established	<ul style="list-style-type: none"> • Stronger statewide IT oversight body established • Powers and duties for statewide direction defined
Early 1990s to late 1990s	Recognition of IT as a strategic state asset	<ul style="list-style-type: none"> • Governor given more control over IT • Development of statewide technical architecture • Establishment of statewide quality assurance policies and processes with increased project visibility • Beginning of statewide coordination through agency IT planning and IRMC strategies and initiatives • Network transformation to TCP/IP and statewide wide area network (WAN)
1999	Senate Bill 222 and House Bill 168	<ul style="list-style-type: none"> • CIO reports to Governor – enterprise approach for managing IT strengthened • Credit card acceptance allowed – beginnings of e-government
Late 1990s to early 2000s	Rise of e-government and increased visibility of costs and potential benefits of IT	<ul style="list-style-type: none"> • Greater control of Governor through CIO • Powers and duties of CIO and ITS codified • Increased central responsibility through CIO • IT purchasing and planning leveraged and streamlined • Increased legislative involvement • Statewide IT initiatives started with implementation of portal and common payment services
2001	Senate Bill 2005	<ul style="list-style-type: none"> • CIO assigned statewide security responsibilities • CIO review of agency IT expansion budget requests

Chapter 3 Analysis of Agency Expansion Budget Requests (Attachment Cs)

October 28, 2002

MEMORANDUM

To: David McCoy, State Budget Officer

From: George Bakolia, State CIO

Subject: State CIO Review of Agency Expansion Budget Requests
 (Attachment Cs) for the 2003 – 2005 Biennium

As directed by G.S. 143-6(b2), the review of agency IT expansion budget funding requests of \$100,000 or greater has been completed. These requests are in the format of Attachment C templates specified in your budget preparation instructions. They have been returned to the agencies, with my recommended disposition and comments, for inclusion in their budget packages. The attached State CIO Review table lists each request by agency, with costs, recommendations, and comments. Amplifying and explanatory information is offered in sections below.

Review Scope and Criteria

My review was conducted primarily from a technology perspective, and the criteria are listed as follows:

- Compatibility with agency IT plans.
- Technically sound (proposed technology is appropriate for meeting business needs and follows the statewide technical architecture, security standards, etc.).
- Financial justification in that the proposed investment is a useful employment of funds for technology, and the funding request appears to be adequate for accomplishing the purpose of the investment.

- Support of the enterprise approach by making use of or adding to the state's common technical services and/or shared technical infrastructure.
- Minimize overlap or duplication among agencies of technical services, infrastructures or applications.
- Compatible with other statewide and/or agency technology initiatives.

While the analysis of each request was thorough, the extent of examination was limited due to time constraints and the realization that opportunities for further more detailed reviews will be forthcoming for proposed investments that are selected for additional consideration. In addition, as indicated by many of my comments on the Attachment Cs, should funding materialize, the IRLC's project certification process offers a checkpoint for the detailed assessment of major project components, including benefits, costs, risks, management, and technology.

Summary Statistics

The key statistics and summarized information for the funding requests are highlighted below.

- In spite of the state's severe budget crisis, the great dependence of state government on technology is confirmed by the submission of 85 Attachment Cs by 13 agencies.
- Agencies recognize the need to provide better and more responsive services to citizens by 21 requests for new applications.
- There is a growing need to address the problem of aging applications, with 17 requests covering the replacement or modernization of legacy systems.
- The ability to support present ongoing obligations is becoming compromised, as indicated by 10 requests for new positions and 3 requests for funds to support current operations.
- Much of the agency technical infrastructure is becoming outdated, obsolete or inadequate to meet current demands, as evidenced by 30 requests for replacement or upgrading of PCs, LAN equipment, data centers, office software, etc.

- The current budgetary approach hampers interagency cooperation and the full adoption of the enterprise approach, since 10 requests address common infrastructure and another 12 are candidates for common shared applications or services.
- The protection of assets, privacy of individuals, and confidentiality of data have been long-term significant considerations for both the statewide and agency management of technology. The greater awareness and increased importance of these items are recognized by the agencies through 2 specific security related requests and the inclusion of this item in requests for modernizing systems and applications to meet security requirements.

IT Plans

IT plans are required to be submitted by the agencies submitting Attachment Cs. The remaining agencies must submit their IT plans to my staff by the middle of next month. Since all agency plans have not been received, and because the review of present plans has been cursory due to time limitations, our observations to date are preliminary in nature. I will provide a report on the agency IT plans to you and the other members of the IRMC for its December meeting.

Conclusion

Technology has become a pervasive component of state government, and it is essential to the ongoing operations of the state's programs and business activities. However, the pernicious effects of a severe and chronic budget crisis and a continuing period of shortfalls in funding are becoming more evident. This leads to two key conclusions:

- The agencies are reaching a limit where their ability to support continuing technical operations is jeopardized. Critical applications are becoming at risk due to aging and outdated hardware and software infrastructures, unsupported and increasingly difficult to maintain legacy code, insufficient staffing resources, lack of security related knowledge and infrastructure, and shortage of funds for telecommunications and computing services.
- The enterprise approach for managing technology must be strengthened and pursued to address agency needs under the foreseeable long-term adverse budget conditions. We must adopt best practice methods for managing agency technical

infrastructures, redistribute and consolidate these assets where cost-effective, standardize hardware/software configurations and aggregate purchasing demand for achieving the best volume discounts, and use to the greatest possible extent statewide shared technical infrastructures and common technical services to realize the greatest economies of scale.

I will be glad to respond to any questions you may have.

Chapter 4 – Analysis of Agency IT Plans

November 21, 2002

MEMORANDUM

To: Members of the IRMC

From: George Bakolia, State CIO

Subject: State CIO Assessment of Agency IT Plans for the 2003 – 2005 Biennium

For the past several months, the agencies have been preparing and submitting expansion budget requests (Attachment Cs) and agency IT plans. My staff has reviewed these documents and prepared summary assessments from a statewide perspective.

The information obtained and knowledge gained from the reviews of the Attachment Cs and the agency IT plans are being used as major inputs for the development of both the agency IT plan for ITS and the Governor and IRMC's Statewide Strategies and Initiatives. A draft of the Statewide Strategies and Initiatives will be submitted to you for your January 2003 meeting.

As you know, last month I reported to you on the findings from the review of Attachment Cs and my certification of them. The objective of this memorandum is to summarize the results of the review of the agency IT plans. As of the date of this memorandum, 21 agencies have submitted IT plans to my staff, and 3 additional agencies have been notified that their plans are expected, but not yet received.

Intent, Scope and Criteria of Review

As agreed with the agencies and the IRMC, my staff's review of agency IT plans is not to be considered an audit of the plans, but as the identification of trends and issues that present major enterprise-level IT policy and/or budgetary issues or concerns. The review was conducted primarily from a technology perspective, and the design of the review is described by the objectives listed as follows:

- Examine the status of the current agency technical infrastructure and management capabilities from the perspective of being able to meet present and future agency missions, business strategies, and program goals and objectives.
- Evaluate the reasonableness and justification of proposed additions, enhancements and other changes to agency technical infrastructures.
- Assess the logic and soundness of business and technical strategies for providing better and more responsive services to the business and program areas and for improving the management of technical investments and operations, including proposed initiatives and projects.
- Identify opportunities for the greater use of the state's common technical services and shared technical infrastructure, as well as the sharing of applications, personnel resources, and management capabilities among multiple agencies.

Summary Findings

Listed below are general themes from the review that are applicable when looking at the state as a whole. Each finding is valid and must be addressed by legislative and senior executive bodies. However, the individual findings do not apply equally to all agencies. Concerns identified by my staff specific to individual agency IT plans are being addressed with the respective agency CIOs.

- IT is an integral part of state government operations, and it must be used appropriately and managed well – IT is a pervasive part of state government; an effective tool for delivering high quality, responsive, and cost-effective services to citizens; and instrumental in improving the performance and accountability of governmental programs and initiatives. However, the tremendous dependency of state government on IT necessitates continuing management attention.
- There continues to be a compelling need for statewide leadership, direction, and technical and managerial assistance – In general, agencies are successful at managing and running the legacy applications that are imperative to their business and program priorities. However, due to limited fiscal and personnel resources,

the following activities are becoming more difficult and risky to accomplish: (a) transition to modern architectures, (b) implementation of new technologies and applications, and (c) operations of increasingly complex technical infrastructures. Similar to what it has done for the implementation of statewide IT projects, the state should develop and publish best practices and appropriate standards to guide agency management and staff in the operations management of IT assets. Equally important, in many situations, short-term and focused hands-on assistance is required to fill in the gaps of skills and numbers of agency staffing to help them solve management issues and technical challenges.

- Expanded purchasing support for IT products and services is requested – Past moves toward a more statewide perspective must continue in the areas of software licensing, hardware procurement, and personnel services. While reasonable agency choice and buying flexibility must be accommodated, current efforts must be continued for receiving maximum volume discounts by improving the aggregation of demand and reducing the number of vendors on contract.
- Planning and implementation assistance is needed to achieve appropriate levels of security – Agencies are treading new ground, with which they have little familiarity, experience, or skills. In addition to developing policies and standards, assistance is necessary to implement the policies and make the standards a reality. Common approaches and standard tools are required, as the in-house expertise is not available for making the transition to an active security program, and funding is limited.
- Agencies need tailored and suitable disaster recovery and business continuity capabilities, especially for distributed IT assets (servers, PCs, etc.) – While mainframe-based applications at ITS are accommodated through the state's contract for remote-site production facilities, the many server-based applications geographically dispersed throughout the state are not covered by adequate disaster recovery plans or capabilities. Some of these are mission-critical, and even short-term losses due to person-made or natural causes could be devastating to citizen service, with attendant negative public relations and adverse political repercussions.
- The lack of adequate personnel resources is a continuing and growing problem, and it is beginning to place applications and

operations at risk – Some agencies are having difficulty transitioning from their legacy-oriented and mainframe-based technical infrastructure to today's distributed-asset and Internet/network-intensive technologies. The current state budget crisis is exacerbating the problem, with the elimination of key positions and the reduction in funds for training. This challenge is compounded by the fact that many agency technical workers are reaching retirement age; therefore, succession planning and knowledge continuity for legacy applications are becoming increasingly important issues. Agencies have been using outsourcing contracts for personnel services to address these situations; however, this approach is not cost-effective, and it ignores the longer-term problem.

- Project management and technical architectures are becoming more acute challenges for the agencies – Agencies are engaging in larger and higher-risk projects. These are more complex technically and present business and organizational complications heretofore not experienced. While they have the potential for offering great value, they also present opportunities for expensive and visible shortcomings. Several agencies are committing staffing resources and adopting the processes and tools to obtain a more consistent and reliable approach to project management. In some cases, additional attention is being focused on the need for the development of agency and applications technical architectures. However, agencies are requesting additional support in the areas of project management and technical architectures to assist them in coping with their new and more involved technical and business environments.

Conclusions

Three major conclusions are presented as follows:

- The state must give IT the necessary funding priority and management attention – from the top to the bottom of its governance and management structure. IT is neither going away nor stagnating - citizens are continuing to ask for new and expanded services, and the taxpayers are demanding more efficient operations and cost-effective programs that are enabled by the use of IT facilities. IT is not self-managed, inexpensive, or simple to control. Rather, it is complex and expensive, and it demands constant interest and requires difficult decision-making. More important, it is not necessarily how much an organization spends on IT that determines the benefits received – it is how the organization uses IT and how it manages IT that counts.
- It appears that the pernicious effects of a severe and chronic budget crisis and the continuing shortfalls in funding for the unforeseen future are being felt within the IT community. This is particularly noticeable in the aging of technical infrastructure, the growth in the backlog for applications development, and the less reliable and more unpredictable operating performance of applications. In addition, the state's budget problem is a primary cause for the inability to obtain and fill technical positions and to provide essential training for IT staff.
- There is no consistent policy for the funding of IT investments or operations in state government, leading to uneven resources, results and benefits among the agencies. While most agencies submitted numerous Attachment Cs for much-needed hardware/software, new or upgraded applications to replace at-risk assets, and even ongoing operating funds, some agencies did not submit any expansion budget requests and indicated in their plans that they may be self-sufficient with present continuation budgets. The age-old gap between the 'haves' and 'have-nots' seems to be expanding, and it will have negative effects on any attempts to implement 'enterprise solutions'.

I will be glad to respond to any questions you may have.